CLAIMS

1. Copy protected digital data comprising
- a passive part (2) comprising content (1) to be protected in encrypted form;
- an active part (3) comprising information (4) how to decrypt the content (1) comprised in the passive part (2); and
- a hidden part (6);

wherein
the active part (3) and the corresponding passive part (2) constitute an active content (8) and
the hidden part (6) is allocated to the active content (8) and/or the active part (3) of the active content (8) and/or the passive part (2) of the active content (8), the hidden part (6) comprising information (7) about properties of the respective active content (8) and/or respective active part (3) and/or the respective passive part (2);
characterised in that
the active part (2) of the active content (8) additionally comprises rules (5) to allow and/or forbid decryption of the content (1) comprised in the passive part (2) of the active content (8) based on the information (7) comprised in the hidden part (6).

2. Copy protected digital data according to claim 1,
characterised in that
the active part (3) is adapted to
- read out the information (7) comprised in the respective hidden part (6),
- compare said information (7) with the rules (5) and
- perform or deny decryption of the content (1) comprised in the passive part (2) based on a comparison result.

3. Copy protected digital data according to claim 1 or 2,
characterised in that
the active part (3) of the active content (8) is adapted to permanently deny decryption of the content (1) comprised in the passive part (2) of the active content (8) if the information (7) comprised in the hidden part (6) does not comply with the rules (5) of the active part (3).

4. Copy protected digital data according to claim 1,2 or 3,
characterised in that

the active part (3) further comprises information (4') how to encrypt decrypted content (1').

5. Copy protected digital data according to one of the preceding claims,
characterised in that
the active part (3) is further adapted to perform decoding and/or reproduction of decrypted content (1') after decryption of the content (1) comprised in the passive part (2).

6. Copy protected digital data according to one of the preceding claims,
characterised in that
the active part (3) is adapted to completely load and delete the passive part (2), to decrypt and reproduce the content (1) comprised in the loaded passive part (2), to encrypt the decrypted content (1') after reproduction and to store the encrypted content (1) into a new passive part (2*).

7. Copy protected digital data according to claim 6,
characterised in that
the active part (3) is adapted to perform loading, deletion, decryption, encryption and storing of the content (1) comprised in the passive part (2) in real time during reproduction of the content (1) comprised in the passive part (2).

8. Copy protected digital data according to claim 6 or 7,
characterised in that
the active part (3) is adapted to store the new passive part (2*) together with an adapted active part (3) into a new active content (8*).

9. Copy protected digital data according to one of the preceding claims,
characterised in that
the active part (3) is adapted to automatically amend itself to build an amended active part (3*) each time decryption and/or encryption of the passive part (2) is performed.

10. Copy protected digital data according to one of the preceding claims,
characterised in that
the active part (3) is a tamper resistant software.

11. Copy protected digital data according to one of the preceding claims,
characterised in that

the rules (5) comprised in the active part (3) comprise information (5') how often the content (1) comprised in the passive part (2) is allowed to be decrypted and how often the content (1) comprised in the passive part (2) has already been decrypted.

12. Copy protected digital data according to one of the preceding claims,
characterised in that
the rules (5) comprised in the active part (3) comprise information (5'') how long the content (1) comprised in the passive part (2) is allowed to be decrypted.

13. Copy protected digital data according to one of the preceding claims,
characterised in that
the rules (5) comprised in the active part (3) comprise information (5''') how often the content (1) comprised in the passive part (2) is allowed to be lend and how often the content (1) comprised in the passive part (2) has already been lend.

14. Copy protected digital data according to one of the preceding claims,
characterised in that
the active content (8) constitutes a data file operable by an operating system.

15. Copy protected digital data according to one of the preceding claims,
characterised in that
the active part (3) is adapted to separate the passive part (2) from the active content (8) for decryption of the content (1) comprised in the passive part (2).

16. Copy protected digital data according to one of the preceding claims,
characterised in that
the hidden part (6) automatically is allocated to the active content (8) and/or the active part (3) of the active content (8) and/or the passive part (2) of the active content (8) by an operating system (9).

17. Copy protected digital data according to one of the preceding claims,
characterised in that
the hidden part (6) is stored in a system file (10) of an operating system (9).

18. Copy protected digital data according to one of the preceding claims,
characterised in that
the hidden part (6) is stored in encrypted form.

19. Copy protected digital data according to one of the preceding claims,

characterised in that
the hidden part (6) further comprises information (7') about the location of the active content (8) and/or the active part (3) of the active content (8) and/or passive part (2) of the active content (8).

20. Copy protected digital data according to one of the preceding claims,
characterised in that
the information (7, 7') comprised in the hidden part (6) automatically is changed by an operating system (9) to build an amended hidden part (6*) each time the active content (8) and/or the active part (3) of the active content (8) and/or the passive part (2) of the active content (8) and/or the content (1) comprised in the passive part (2) of the active content (8) is read out and/or amended and/or stored.

21. Copy protected digital data according to one of the preceding claims,
characterised in that
the encrypted content (1) comprised in the passive part (2) is digitised audio data and/or digitised video data and/or digitised picture date and/or a database and/or a software and/or digitised text.

22. Recording medium (11) or consumer electronic device or personal computer comprising copy protected digital data according to one of the preceding claims.

23. Method of reproducing a copy protected digital data comprising
- a passive part (2) comprising content (1) to be protected in encrypted form;
- an active part (3) comprising information (4) how to decrypt the content (1) comprised in the passive part (2); and
- a hidden part (6);
wherein
the active part (3) and the corresponding passive part (2) constitute an active content (8),
the hidden part (6) is allocated to the active content (8) and/or the active part (3) of the active content (8) and/or the passive part (2) of the active content (8), the hidden part (6) comprising information (7) about properties of the respective active content (8) and/or respective active part (3) and/or the respective passive part (2), and
the active part (3) of the active content (8) further comprises rules (5) to allow and/or forbid decryption of the content (1) comprised in the passive part (2) of the active content (8) based on the information (7) comprised in the hidden part (6);
the method comprising the following steps:

- (S1) reading out the information (7) comprised in the hidden part (6) of the copy protected digital data;
- (S2) comparing said information (7) with the rules (5) comprised in the corresponding active part (3) of the active content (8);
- (S3) denying decryption of the content (1) comprised in the passive part (2) of the active content (8) if the information (7) read out from the hidden part (6) does not comply with the rules (5) and terminating the method;
- (S4) loading the encrypted content (1) comprised in the passive part (2) of the active content (8) if the information (7) read out from the hidden part (6) complies with the rules (5);
- (S5) performing decryption of the encrypted content (1); and
- (S6) reproducing decrypted content (1').

24. Method according to claim 23,
characterised in that the method further comprises the steps of
- (S7) deleting the passive part (2);
- (S8) encrypting the decrypted content (1') after reproduction; and
- (S9) storing the encrypted content (1) into a new passive part (2*).

25. Method according to claim 24,
characterised in that
the step (S6) of reproducing the decrypted content (1'), the step (S7) of deleting the passive part (2) and the step (S8) of encrypting the decrypted content (1') after reproduction are performed in real time during reproduction of the decrypted content (1').

26. Method according to claim 23 24or 25,
characterised in that the method further comprises the step of
- (S10) automatically amending the hidden part (6) by control of an operating system (9) to built an amended hidden part (6*) each time the active content (8) and/or the active part (3) of the active content (8) and/or the passive part (2) of the active content (8) and/or the content (1) comprised in the passive part (2; 2*) of the active content (8) is read and/or amended and/or stored.

27. Method according to claim 23, 24, 25 or 26,
characterised in that the method further comprises the step of
- (S11) automatically amending the active part (3) of the active content (8) by control of the active part (3) of the active content (8) to build an amended active

part (3*) each time decryption of the content (1) comprised in the passive part (2) is performed.

28. Software product comprising a series of state elements which are adapted to be processed by a data processing means such, that a method according to one of the claims 23 to 27 may be executed thereon.